# VERIFYING A NODE ON A NETWORK

This invention relates to the field of communications security, and in particular, to a system and method that verifies the proximity of a node on a network.

Network security can often be enhanced by distinguishing between 'local' nodes and 'remote' nodes on the network. Local nodes, for example, are typically located within a particular physical environment, and it can be assumed that users within this physical environment are authorized to access the network. Remote nodes, on the other hand, are susceptible to unauthorized physical access. Additionally, unauthorized intruders on a network typically access the network remotely, via telephone or other communication channels. Because of the susceptibility of the network to unauthorized access via remote nodes, network security can be enhanced by imposing stringent security measures, or access restrictions, on remote nodes, while not encumbering local nodes with this same restrictions.

It is an object of this invention to provide a system and method that facilitates a determination of whether a node on a network is local or remote. It is a further object of this invention to provide a system and method that facilitates a secure determination of whether a node on a network is local or remote. It is a further object of this invention to integrate this determination with a system or method that verifies the authenticity of the node on the network.

These objects and others are achieved by a system and method that includes timing parameters within a node-verification protocol, such as the Open Copy Protection System (OCPS), to facilitate a determination of the proximity of a target node to a source node. The node-verification protocol includes a query-response sequence, wherein the source node communicates a query to the target node, and the target node communicates a corresponding response to the source node. The source node establishes a lower bound on the distance between the source node and the target node, based on a measure of the time required to effect this query-response sequence. The time required to effect this sequence includes the time required to communicate the query and response, as well as the time required to process the query and generate the response. The target node includes a measure of the time required to process the query and generate the response to the source node. The source node subtracts this time from the total query-response time to determine

the time consumed for the communication. This communication time is compared to a threshold value to determine whether the target node is local or remote relative to the source node.

FIG. 1 illustrates an example block diagram of a network of nodes.

FIG. 2 illustrates an example block diagram of a source and target node that effect a query-response protocol in accordance with this invention.

Throughout the drawings, the same reference numeral refers to the same element, or an element that performs substantially the same function.

FIG. 1 illustrates an example block diagram of a network 150 of nodes 110. One of the nodes, NodeD 110, is illustrated as being distant from the other nodes 110. In accordance with this invention, each of the nodes 110 is configured to be able to determine the proximity of each other node 110. In a typical embodiment of this invention, the proximity determination is limited to a determination of whether the other node is "local" or "remote", although a more detailed determination of distances can be effected using the techniques disclosed herein.

FIG. 2 illustrates an example block diagram of a source node 110S and target node 110T that effect a query-response protocol to determine the proximity of the target node 110T to the source node 110S in accordance with this invention. The source node 110S includes a processor 210 that initiates a query, and a communications device 220 that transmits the query to the target node 110T. The target node 110T receives the query and returns a corresponding response, via its communications device 230. To assure that the response corresponds to the communicated query, the protocol calls for the target node 110T to process at least a portion of the query and to include a result of this processing in the response, via a processor 240.

The source node 110S is configured to measure the time consumed by the query-response process, illustrated in FIG. 2 as $T_{query\text{-}response}$ 280. This query-response time 280 includes the time to communicate the query and response, $T_{communicate}$ 260, as well as the time to process the query and generate the response at the target node 110T, $T_{process}$ 270. In accordance with this invention, the target node 110T is configured to include a measure of this processing time 270 within the response provided to the source node 110S. The source node 110S subtracts the processing time 270 from the query-response time 280 to determine the communication time 260. Using known techniques, the distance between the

source 110S and target 110T can be calculated using this determined communication time 260. As noted above, in a typical embodiment, the communication time 260 is used to determine whether the target 110T is local or remote from the source 110S. This determination is made in a preferred embodiment of this invention by comparing the communication time 260 to a nominal threshold value, typically not more than a few milliseconds. If the communication time 260 is below the threshold, the target 110T is determined to be local; otherwise, it is determined to be remote.

In a typical embodiment, the source 110S uses the remote/local proximity determination to control subsequent communications with the target 110T. For example, some files may be permitted to be transferred only to local nodes, all communications with a remote node may be required to be encrypted, and so on. Optionally, multiple threshold levels may be defined to distinguish different ranges of distances, such as whether a remote target node is located within the same country as the source node, and so on.

Note that an unauthorized node can subvert the above process by providing a false processing time. In a preferred embodiment of this invention, the above query-response process is integrated within a node-authentication process, such as a key-exchange process, which typically includes one or more query-response sequences. By integrating the query-response process within the node-authentication process, the reported processing time is verified as being authentic.

The OCPS protocol, for example, includes an authentication stage, a key exchange stage, a key generation phase, and subsequent data transmission phases. The key exchange phase is effected via a modified Needham-Schroeder key exchange protocol, as described in "Handbook of Applied Cryptography", Menezes et al.

At the authentication stage, each of the source 110S and target 110T nodes authenticates a public key of each other.

At the start of the key exchange phase, the source 110S encrypts a random number and a random key, using the public key of the target 110T, and transmits both encryptions to the target 110T. In accordance with this invention, the source node 110S initiates a timer when these encryptions are transmitted to the target 110T.

The target 110T decrypts the random number and random key, using the private key of the target. The target 110T generates a new random number and a new random key, and encrypts the new random number, the new random key, and the decrypted random

number from the source 110S, using the public key of the source 110S, to form a response that is to be communicated to the source 110S. The target 110T optionally signs the response, using the target's private key. In accordance with this invention, the target 110T also includes a measure of the time required to effect the decryption, encryption, and signing within the signed response. This processing time is optionally encrypted using the public key of the source. Because this decryption, encryption, and signing process generally consumes the same amount of time at a given target node, the target node is preferably configured to provide a predefined processing time as the measure of time to effect this processing. By signing the response, the target 110T binds the reported processing time to the other parameters in the current response, thereby precluding an unauthorized replacement of the encrypted processing time with an alternative time that is encrypted using the public key of the source 110S.

When the source node 110S receives the response, it terminates the aforementioned timer. The source node 110S verifies the signed message, using the public key of the target 110T, and decrypts the random numbers and random key from the response, using the private key of the source 110S. If the processing time within the response is encrypted, it is also decrypted at this time by the source 110S, using the private key of the source 110S. In accordance with this invention, the source 110S subtracts the processing time from the time duration measured by the timer between the transmission of the encrypted query from the source 110S and the reception of the encrypted response from the target 110T to determine the round-trip communication time between source 110S and target 110T.

To confirm the key exchange, the source 110S transmits the decrypted new random number back to the target 110T. Both the source 110S and target 110T control subsequent communications based upon receipt of the proper decrypted random numbers. In accordance with this invention, the source 110S also controls subsequent communications based upon the determined communication time.

If both nodes are verified, subsequent communications between the source 110S and target 110T encrypt the communications using a session key that is a combination of the random keys, the public keys, and a session index.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention

and are thus within its spirit and scope. For example, in the above described OCPS protocol, the target node 110T may also be configured to determine the proximity of the source node 110S, by timing the process between the transmission of the encrypted response and the receipt of the decrypted random number from the source 110S. In this embodiment, the source 110S is configured to include a measure of the time required to process the encrypted response and transmit the decrypted random number in the last key exchange message that includes the decrypted random number, digitally signed by the source 110S. The target 110T subtracts this processing time from its measured time between transmission and receipt to determine the round-trip target-source-target communication time, and thus the proximity of the source 110S to the target 110T. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.